

**Article 7.1.**  
**Computer Crimes.**

**§ 18.2-152.1. Short title.**

This article shall be known and may be cited as the "Virginia Computer Crimes Act."

(1984, c. 751.)

**§ 18.2-152.2. Definitions.**

For purposes of this article:

*"Computer"* means an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.

*"Computer data"* means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. "Computer data" may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

*"Computer network"* means two or more computers connected by a network.

*"Computer operation"* means arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. A "computer operation" for a particular computer may also be any function for which that computer was generally designed.

*"Computer program"* means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations.

*"Computer services"* means computer time or services, including data processing services,

Internet services, electronic mail services, electronic message services, or information or data stored in connection therewith.

*"Computer software"* means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

*"Electronic mail service provider" (EMSP)* means any person who (i) is an intermediary in sending or receiving electronic mail and (ii) provides to end-users of electronic mail services the ability to send or receive electronic mail.

*"Financial instrument"* includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof.

*"Network"* means any combination of digital transmission facilities and packet switches, routers, and similar equipment interconnected to enable the exchange of computer data.

*"Owner"* means an owner or lessee of a computer or a computer network or an owner, lessee, or licensee of computer data, computer programs, or computer software.

*"Person"* shall include any individual, partnership, association, corporation or joint venture.

*"Property" shall include:*

1. Real property;
2. Computers and computer networks;
3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
  - a. Tangible or intangible;
  - b. In a format readable by humans or by a computer;
  - c. In transit between computers or within a computer network or between any devices which comprise a computer; or
  - d. Located on any paper or in any device on which it is stored by a computer or by a human; and
4. Computer services.

A person "uses" a computer or computer network when he attempts to cause or causes:

1. A computer or computer network to perform or to stop performing computer operations;
2. The withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or
3. A person to put false information into a computer.

A person is "without authority" when he has no right or permission of the owner to use a computer or computer network or he uses a computer or computer network in a manner exceeding such right or permission.

(1984, c. 751; 1999, cc. 886, 904, 905; 2000, c. 627; 2003, cc. 987, 1016.)

### **§ 18.2-152.3. Computer fraud.**

Any person who uses a computer or computer network without authority and with the intent to:

1. Obtain property or services by false pretenses;
2. Embezzle or commit larceny; or
3. Convert the property of another

is guilty of the crime of computer fraud.

If the value of the property or services obtained is \$200 or more, the crime of computer fraud shall be punishable as a Class 5 felony. Where the value of the property or services obtained is less than \$200, the crime of computer fraud shall be punishable as a Class 1 misdemeanor.

(1984, c. 751; 1985, c. 322; 2003, cc. 987, 1016.)

#### **§ 18.2-152.3:1. Transmission of unsolicited bulk electronic mail (spam); penalty.**

A. Any person who:

1. Uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers; or

2. Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling

the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information is guilty of a Class 1 misdemeanor.

B. A person is guilty of a Class 6 felony if he commits a violation of subsection A and:

1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or

2. The revenue generated from a specific UBE transmission exceeded \$1,000 or the total revenue generated from all UBE transmitted to any EMSP exceeded \$50,000.

C. A person is guilty of a Class 6 felony if he knowingly hires, employs, uses, or permits any minor to assist in the transmission of UBE in violation of subdivision B 1 or subdivision B 2.

(2003, cc. 987, 1016.)

#### **§ 18.2-152.4. Computer trespass; penalty.**

A. It shall be unlawful for any person to use a computer or computer network without authority and with the intent to:

1. Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network;

2. Cause a computer to malfunction, regardless of how long the malfunction persists;

3. Alter or erase any computer data, computer programs, or computer software;

4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;

5. Cause physical injury to the property of another; or

6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.

7. [Repealed].

B. Any person who violates this section shall be guilty of computer trespass, which offense shall be

punishable as a Class 1 misdemeanor. If there is damage to the property of another valued at \$2,500 or more caused by such person's malicious act in violation of this section, the offense shall be punishable as a Class 6 felony.

C. Nothing in this section shall be construed to interfere with or prohibit terms or conditions in a contract or license related to computers, computer data, computer networks, computer operations, computer programs, computer services, or computer software or to create any liability by reason of terms or conditions adopted by, or technical measures implemented by, a Virginia-based electronic mail service provider to prevent the transmission of unsolicited electronic mail in violation of this article. Nothing in this section shall be construed to prohibit the monitoring of computer usage of, the otherwise lawful copying of data of, or the denial of computer or Internet access to a minor by a parent or legal guardian of the minor.

(1984, c. 751; 1985, c. 322; 1990, c. 663; 1998, c. 892; 1999, cc. 886, 904, 905; 2002, c. 195; 2003, cc. 987, 1016.)

#### **§ 18.2-152.5. Computer invasion of privacy.**

A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

B. The crime of computer invasion of privacy shall be punishable as a Class 1 misdemeanor.

(1984, c. 751; 1985, c. 398; 2001, c. 358.)

#### **§ 18.2-152.6. Theft of computer services.**

Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services, which shall be punishable as a Class 1 misdemeanor. If the theft of computer services is valued at \$2,500 or more, he is guilty of a Class 6 felony.

(1984, c. 751; 1985, c. 322; 2003, cc. 987, 1016.)

#### **§ 18.2-152.7. Personal trespass by computer.**

A. A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network without authority and with the intent to cause physical injury to an individual.

B. If committed maliciously, the crime of personal trespass by computer shall be punishable as a Class 3 felony. If such act is done unlawfully but not maliciously, the crime of personal trespass by computer shall be punishable as a Class 6 felony.

(1984, c. 751; 1985, c. 322; 2003, cc. 987, 1016.)

**§ 18.2-152.7:1. Harassment by computer; penalty.**

If any person, with the intent to coerce, intimidate, or harass any person, shall use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act, he shall be guilty of a Class 1 misdemeanor.

(2000, c. 849.)

**§ 18.2-152.8. Property capable of embezzlement.**

For purposes of § 18.2-111, personal property subject to embezzlement shall include:

1. Computers and computer networks;
2. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
  - a. Tangible or intangible;
  - b. In a format readable by humans or by a computer;
  - c. In transit between computers or within a computer network or between any devices which comprise a computer; or
  - d. Located on any paper or in any device on which it is stored by a computer or by a human; and
3. Computer services.

(1984, c. 751.)

**§ 18.2-152.9. Limitation of prosecution.**

Notwithstanding the provisions of § 19.2-8, prosecution of a crime which is punishable as a misdemeanor pursuant to this article must be commenced before the earlier of (i) five years after the commission of the last act in the course of conduct constituting a violation of this article or (ii) one year after the existence of the illegal act and the identity of the offender are discovered by the Commonwealth, by the owner, or by anyone else who is damaged by such violation.

(1984, c. 751.)

**§ 18.2-152.10. Venue for prosecution.**

For the purpose of venue under this article, any violation of this article shall be considered to have been committed in any county or city:

1. In which any act was performed in furtherance of any course of conduct which violated this article;
2. In which the owner has his principal place of business in the Commonwealth;
3. In which any offender had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, computer data, or other material or objects which were used in furtherance of the violation;
4. From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;
5. In which the offender resides; or
6. In which any computer which is an object or an instrument of the violation is located at the time of the alleged offense.

(1984, c. 751; 1985, c. 322.)

**§ 18.2-152.11. Article not exclusive.**

The provisions of this article shall not be construed to preclude the applicability of any other provision of the criminal law of this Commonwealth which presently applies or may in the future apply to any transaction or course of conduct which violates this article, unless such provision is clearly inconsistent with the terms of this article.

(1984, c. 751.)

**§ 18.2-152.12. Civil relief; damages.**

A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

B. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, the injured person, other than an electronic mail service provider, may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover the lesser of \$10 for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or \$25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

C. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, an injured electronic mail service provider may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover \$1 for each and every intended recipient of an unsolicited bulk electronic mail message where the intended recipient is an end user of the EMSP or \$25,000 for each day an attempt is made to transmit an unsolicited bulk electronic mail message to an end user of the EMSP. In calculating the statutory damages under this provision, the court may adjust the amount awarded as necessary, but in doing so shall take into account the number of complaints to the EMSP generated by the defendant's messages, the defendant's degree of culpability, the defendant's prior history of such conduct, and the extent of economic gain resulting from the conduct. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

D. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party and in such a way as to protect the privacy of nonparties who complain about violations of this section.

E. The provisions of this article shall not be construed to limit any person's right to pursue any



additional civil remedy otherwise allowed by law.

F. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1. In actions alleging injury arising from the transmission of unsolicited bulk electronic mail, personal jurisdiction may be exercised pursuant to § 8.01-328.1.

(1984, c. 751; 1985, c. 92; 1999, cc. 886, 904, 905; 2003, cc. 987, 1016.)

#### **§ 18.2-152.13. Severability.**

If any provision or clause of this article or application thereof to any person or circumstances is held to be invalid, such invalidity shall not affect other provisions or applications of this article which can be given effect without the invalid provision or application, and to this end the provisions of this article are declared to be severable.

(1984, c. 751.)

#### **§ 18.2-152.14. Computer as instrument of forgery.**

The creation, alteration, or deletion of any computer data contained in any computer or computer network, which if done on a tangible document or instrument would constitute forgery under Article 1 (§ 18.2-168 et seq.) of Chapter 6 of this Title, will also be deemed to be forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to any crime set forth in Article 1 (§ 18.2-168 et seq.) of Chapter 6 of this Title if a creation, alteration, or deletion of computer data was involved in lieu of a tangible document or instrument.

(1984, c. 751; 1985, c. 322.)

#### **§ 18.2-152.15. Encryption used in criminal activity.**

Any person who willfully uses encryption to further any criminal activity shall be guilty of an offense which is separate and distinct from the predicate criminal activity and punishable as a Class 1 misdemeanor.

*"Encryption"* means the enciphering of intelligible data into unintelligible form or the deciphering of unintelligible data into intelligible form.

(1999, c. 455.)

**§ 18.2-152.16.**

Repealed by Acts 2004, c. 995.